Issues List for Security Assertion Markup Language (SAML) V2.0

Draft 1~~2~~3, ~~29 June~~ 20 July 2004

Document identifier:

sstc-saml-2.0-issues-draft-1~~2~~3

Location:

http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

Editor:

Eve Maler, Sun Microsystems (eve.maler@sun.com)

Abstract:

This document catalogues issues for Security Assertion Markup Language (SAML) V2.0, which is developed by the OASIS Security Services Technical Committee. It is intended to record specific issues that potentially need to be implemented as changes or additions to a SAML specification. Also see the SAML V2.0 work items document, which provides information on the overall scope of the V2.0 effort and general work items that have been adopted.

Status:

This document is a non-normative working document of the OASIS Security Services Technical Committee. It is not a formal part of the SAML specification suite. The intention is to update it frequently until V2.0 is completed. **See the Revision History for details of changes made in this revision.**

Committee members should send comments on this specification to the security-services@lists.oasis-open.org list. Others should subscribe to and send comments to the security-services-comment@lists.oasis-open.org list. To subscribe, send an email message to security-services-comment-request@lists.oasis-open.org with the word "subscribe" as the body of the message.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Security Services TC web page (http://www.oasis-open.org/committees/security/).

Table of Contents

Table of Issues

1 Introduction

This document catalogues issues for Security Assertion Markup Language (SAML) V2.0, which is developed by the OASIS Security Services Technical Committee. It is intended to record specific issues that potentially need to be implemented as changes or additions to a SAML specification. Also see the SAML V2.0 work items document, which provides information on the overall scope of the V2.0 effort and general work items that have been adopted.

Each issue includes the following information:

- A unique *issue ID*, such as TECH-42. This appears in the section heading. The possible categories are **OVER** for the technical overview, **CORE** for the assertions and protocol and their governing schemas, **BIND** for bindings and profiles, **META** for the metadata exchange format and protocol, **TECH** for other technical issues, **OUT** for the outreach materials, and **MISC** for all other issues.
- A *short name* for the issue. This appears in the section heading.
- The issue's *status*. This appears in the section heading. The possible statuses are **Open** for issues that still need a resolution, **Deferred** for issues that we have put off dealing with until the next version of SAML, **Resolved** for issues that we have resolved but that remain to be implemented, and **Closed** for issues that have a resolution and require no further action (for example, because the resolution has been implemented or because no action at all is necessary).
- The *source* of the issue, indicating where it was first raised or reported.
- The assigned *owner* of the issue. This person is responsible for proposing options and a preferred resolution.
- An arbitrarily long *description* of the issue, including any discussion history.
- Numbered *options* for resolving the issue, as appropriate.
- The *resolution* of the issue, once this information is available. It should include the date and circumstances of the resolution.

2 Technical Deliverable Issues

The following are issues related to the SAML V2.0 technical deliverables.

2.1 CORE: Assertions, Protocol, and Schema Issues

The following are issues related to the assertions and protocol and their governing schemas.

CORE-1 Remove AuthorityBinding Element (*Closed*)

Source:

oasis-sstc-saml-core-1.1.pdf lines 746-747.

Owner:

Eve Maler.

Description:

This impacts the core spec and the assertion schema. Section 2.4.3, Element `<AuthenticationStatement>`, needs to change to remove mention of `<AuthorityBinding>` from the text and the schema snippet and to note the element's removal in a comment, Section 2.4.3.2, Element `<AuthorityBinding>`, needs to be removed, and the assertion schema needs to change correspondingly.

Resolution:

This is a backwards-incompatible change decided and promised in the V1.0 timeframe but unable to be implemented until V2.0. Implemented in core-01.

CORE-2 Remove RespondWith Element (*Closed*)

Source:

oasis-sstc-saml-core-1.1.pdf lines 1012-1013.

Owner:

Eve Maler.

Description:

This impacts the core spec and the assertion schema. Section 3.2.1, Element Complex Type RequestAbstractType, needs to change to remove mention of `<RespondWith>` from the text and the schema snippet and to note the element's removal in a comment, Section 3.2.1.1, Element `<RespondWith>`, needs to be removed, and the assertion schema needs to change correspondingly.

Resolution:

This is a backwards-incompatible change promised in the V1.0 timeframe but unable to be implemented until V2.0. Implemented in core-01.

CORE-3 Remove Deprecated NameIdentifier URIs (*Closed*)

Source:

oasis-sstc-saml-core-1.1.pdf lines 1949-1951.

Owner:

Eve Maler.

Description:

This impacts the core spec. Section 7.3, NameIdentifier Format Identifiers, needs to change to merely mention that a few URIs have been deprecated in this version, and Sections 7.3.2 through 7.3.4, Email Address through Windows Domain Qualified Name, need to winnow down the URI choices to just the recommended URI in each case.

Resolution:

This is a backwards-incompatible change decided and promised in the V1.0 timeframe but unable to be implemented until V2.0. Implemented in core-01.

CORE-4 Require URI References to Be Absolute (*Closed*)

Source:

oasis-sstc-saml-core-1.1.pdf line 219.

Owner:

Eve Maler.

Description:

This impacts the core spec. Section 1.2.1, String and URI Values, needs to change to say “all URI reference values ... and are REQUIRED to be absolute [RFC 2396].” rather than “... strongly RECOMMENDED ...”.

Resolution:

This is a backwards-incompatible change decided in the V1.0 timeframe but unable to be implemented until V2.0. Implemented in core-01.

CORE-5 Null Attribute Values (*Closed*)

Source:

David Warren on the saml-dev list (see thread at http://lists.oasis-open.org/archives/saml-dev/200309/msg00000.html).

Owner:

Rob Philpott.

Description:

How should an implementation send an empty value (i.e. like a NO-VALUE value in a database) for an attribute?

Options:

A number of reasonable options have already been proposed in the email thread.

Resolution:

This has been implemented in core-05 as follows: If the attribute exists but has no value, then the <AttributeValue> element MUST be omitted.” It was later revised as follows: “If the attribute exists but has no value, then the `<AttributeValue>` element MUST be omitted.”

CORE-6 Assertion-Level Subject (*Closed*)

Source:

Conor Cahill on the security-services list (see thread at http://lists.oasis-open.org/archives/security-services/200310/msg00135.html).

Owner:

Scott Cantor, Eve Maler

Description:

When all statements within an assertion have the same subject, is it possible to factor out that subject information and provide it instead at the assertion level? The thinking is that it is extremely inefficient to have to do subject confirmation processing for each statement individually, when the typical (only?) use case is for the same subject to apply to all statements.

Options:

Conor lists two possibilities:

- Add an <Assertion>-level <Subject> element that applies to all statements without a <Statement>-level <Subject>.

- Barring this, add a subject reference mechanism so that a statement could refer to the <Subject> in another statement.

Resolution:

A largely complete solution has been implemented in core-07. At the March 2004 F2F meeting, we made the final decisions on how to support assertion-level-only subjects, along with support for subjectless assertions according to XACML's needs.

CORE-7 SOAP Version in Protocol Binding (*Closed*)

Source:

Scott Cantor, comment at SAML F2F 22-24 October 2003.

Owner:

Scott Cantor

Description:

The current protocol binding to SOAP is based on SOAP V1.1, but now SOAP V1.2 has been published as a W3C Recommendation. Should we use it? Concerns have been expressed about SOAP V1.2's inability to do signatures properly.

Options:

The obvious options are:

1. Leave the binding as it is. This is currently the sentiment of the group.
2. Change the current binding to use SOAP V1.2.
3. Keep the current binding and add an additional binding to SOAP V1.2.

There may be additional actions needed based on the fact that the protocol is being extended to encompass the newn identity federation features. In the cases of options 2 and 3, the security considerations may be impacted.

Resolution:

We confirmed the selection of option #1 in the SSTC telecon of 22 June 2004.

CORE-8 Signing Assertions vs. Responses (*Closed*)

Source:

SAML F2F 22-24 October 2003.

Owner:

Scott Cantor

Description:

Currently we advise signing the whole response rather than individual assertions, but this is too inflexible to allow for the passing through of assertions from elsewhere (“the intermediary problem”). We need to consider the signing of individual assertions.

Options:

N/A

Resolution:

The new SSO profile allows for assertion signing. This is closed.

CORE-9 Wildcarding and Extensibility in the SAML Schemas (~~*Open*~~*Closed*)

Source:

SAML telecon of 28 October 2003, as part of the discussion of the nameid-05 proposal.

Owner:

Eve Maler, Scott Cantor

Description:

Currently, the SAML assertion and protocol schemas allow for type-based extensibility, but have so far been extremely judicious about XML markup extensibility features that do not require the definition of derived types in an extension schema. Although NameIdentifier URIs – for example – provide extensibility of element string content, the schemas have no `<xsd:anyAttribute>` and few `<xsd:any>` wildcards.

Should we be adding `<xsd:anyAttribute>` everywhere on principle? Should we be adding `<xsd:any>` to additional (or all) complex types? This issue came up again in the March-April 2004 F2F because of a comment received from Anne Anderson on the W-28a attribute work.

Options:

The options have been outlined in the schema extensibility paper (latest revision is at http://www.oasis-open.org/committees/download.php/5227/sstc-maler-schema-extension-02-diff.pdf), and actions have been taken on the recommendations therein. There is only a little more work to be done to close out this issue.

Resolution:

Small changes related to schema extensibility have been done in an ongoing manner~~; these will all be documented in future versions of the position paper~~. We agreed in the telecon of 13 July 2004 to close this issue and not to update the position paper, treating it as historical. On the issue of "must ignore", SAML has no such flag, so all extensions are implicitly ignorable, but we need to make this more explicit in the various places that describe extensions.

CORE-10 Fix Description of Evidence Element's Contents (*Closed*)

Source:

Frederic Deleon on saml-dev list (http://lists.oasis-open.org/archives/saml-dev/200310/msg00001.html)

Owner:

Eve Maler

Description:

The description of the contents of the `<Evidence>` element is incorrect. The schema allows an unbounded number of `<AssertionIDReference>` and `<Assertion>` elements in any order, but the description says that it can contain only one subelement.

Options:

Correct the description on lines 912-917 in oasis-sstc-saml-core-1.1 to reflect the correct occurrence of these subelements.

Resolution:

Implemented in sstc-saml-core-2.0-draft-02 (still to be released at the time of publishing this rev-05 issues list).

CORE-11 Validity Period of Identifiers (*Closed*)

Source:

SAML F2F meeting 3-5 February 2004, Hal/Scott discussion on work item W-2

Owner:

Scott Cantor

Description:

The new NotBefore and NotOnOrAfter attributes on the new NameIdentifierAbstractType may not be effective/necessary, depending on what happens with our W-2 (Session Support) solution. Indicating the time of encryption when you don't have integrity protection above that level doesn't do you any good. And providing a validity period for transient name identifiers may not be necessary. However, some think there may be use cases for keeping the attributes anyway.

We now allow for assertions that contain a subject element and no statements. If you want to

issue an identifier that is time-limited, you can create an assertion with just a subject and the relevant conditions, which meets the use case Scott was concerned about in a generic way (which he would need to profile for his purposes).

Options:

It has been suggested that what should appear when you decrypt the identifier is an assertion.

Resolution:

In the 27 April 2004 telecon, we agreed that this issue is closed because the core spec now enables the needed ability. Prateek plans to write up a separate but related issue.

CORE-12 Consider Changing Name Identifier Format Default for Issuer (*Closed*)

Source:

SAML F2F meeting 3-5 February 2004, discussion on work item W-28d

Owner:

Scott Cantor

Description:

Currently, the default (not enforced in the schema) is the “unspecified” URI. Should it be “entity”? Something else?

Resolution:

It was agreed to change the default to “entity”.

CORE-13 Use of Non-Federated Identifiers in Name Identifier Registration Protocol (*Closed*)

Source:

SAML F2F meeting 3-5 February 2004, discussion on work item W-2

Owner:

Scott Cantor

Description:

How do you ensure that the kind of identifier supplied when requesting a federated new one is compatible?

Options:

Either we could allow non-federated identifiers in unrestricted fashion, or allow them in some kind of restricted fashion, or disallow them entirely. The core-08 language proposes disallowing them entirely.

Resolution:

In the March-April 2004 F2F, we agreed that disallowing them serves no purpose, and allowing them doesn't require any restrictions. The relevant paragraph will simply be deleted in core-09.

CORE-14 Indicating the Authority Binding (*Closed*)

Source:

SAML F2F meeting 3-5 February 2004, discussion on work item W-19, HTTP-Based Assertion Referencing

Owner:

Scott Cantor

Description:

The WSS TC will need our advice on how to indicate the location of an authority (along with the assertion ID), now that we've yanked the AuthorityBinding attribute.

Resolution:

As of the 11 May 2004 telecon, we decided to close this issue with no action. Ron Monzillo reported that "All we [the WSS TC] need is a URI that identifies where to go and what assertion to get. The SAML token profile uses the notion of an authority binding; it will switch to URIs as soon as it gets revved to a SAML V2.0 basis."

CORE-15 Health Warning on xsi:type Extensions of AttributeValue (*Closed*)

Source:

SAML F2F meeting 3-5 February 2004, discussion on work item W-28a*

Owner:

Eve Maler

Description:

It was noted that using xsi:type on AttributeValue in order to further constrain its contents (from xs:anyType to some specific type) can result in problems because xsi:type requires that the extension schema be present. We agreed that we should add a note to the core spec warning people about this.

Resolution:

The TC agreed to do this at the F2F. Implemented in core-08. "**Note:** Specifying a datatype on `<AttributeValue>` using `xsi:type` will require the presence of the extension schema that defines the datatype in order for schema processing to proceed."

CORE-16 Inconsistent Naming (*Closed*)

Source:

Mail message reviewing core-06 changes: http://lists.oasis-open.org/archives/security-services/200402/msg00156.html

Owner:

Eve Maler

Description:

"SAML previously used long names; Liberty shortened some for efficiency reasons. So we now have <AuthenticationStatement> but <AuthnRequest>, and <NameIdentifier> but NameIDPolicy. We need to decide whether (a) the inconsistency is okay, (b) if not, which way we go for what reasons, and (c) whether we want to do a full-on succinctness assault."

Options:

Following are some ideas about places to shorten names, if we decide to shorten across the board:

1. Identifier becomes ID: various old element names would become BaseID, NameID, SPProvidedID, EncryptedID, NewID, RegisterNameIDRequest, RegisterNameIDResponse, NameIDMappingRequest, NameIDMappingResponse (note that we already have AssertionIDReference, AssertionID, RequestID, ResponseID), and the corresponding types would do the same
2. ID attributes become simply ID: old names AssertionID, RequestID, ResponseID all become ID (AssertionConsumerServiceID and RequesterID should stay the same since it's not the ID of the element it's on; IDPEntry has an ID attribute of type anyURI, so maybe this name should change entirely)
3. Authentication becomes Authn: various old element names would become AuthnStatement, AuthnMethod, AuthnInstant, AuthnQuery (note that we already have AuthnContext, AuthnContextClassRef, AuthnContextStatement, AuthnContextStatementRef, AuthnRequest, RequestAuthnContext, ForceAuthn, and the type name AuthnContextComparisonType), and the corresponding types would do the same
4. Authorization becomes Authz: various old element names would become

AuthzDecisionStatement, AuthzDecisionQuery, and the corresponding types would do the same

5. Subelements and attributes of an element would lose any duplicated prefixes or suffixes: SubjectConfirmation would contain Method and Data rather than prefixed versions of same; the subelements of Conditions would not repeat the word Condition in their names; the elements inside AuthnContext would not start with AuthnContext; inside StatusCode would appear simply Message and Detail

There are probably other opportunities not listed here.

In the 11 May 2004 telecon, it was pointed out that because SAML uses global elements, perhaps it's better not to remove “redundant” prefixes as suggested in #5 above. It was also pointed out that shortening “Confirmation” to “Conf” and undertaking other similar truncations would be useful. We will consider these ideas shortly.

Resolution:

In the 11 May 2004 telecon, the suggestions above were taken one by one. The following decisions were made so far:

- PASSED: In element names and their corresponding type names, s/Identifier/ID/
- PASSED: In attribute names, s/.*ID/ID/ (but see also issue CORE-26 below)
- PASSED: In element names, attribute names, and any corresponding type names, s/Authentication/Authn/ and ensure that any cases of just “Auth” (with no “entication” or “n”) that refer to authentication get the “n” added
- PASSED: In element names, attribute names, and any corresponding type names, s/Authorization/Authz/

We decided on the 22 June 2004 telecon to consider this closed.

CORE-17 Bag of Conditions (*Closed*)

Source:

Mail message reviewing core-06 changes: http://lists.oasis-open.org/archives/security-services/200402/msg00156.html

Owner:

Eve Maler

Description:

“The proposal for the new <ProxyRestrictionCondition> brings to light an old SAML ugliness: <Conditions> contains a repeatable bag of subelements, necessitating verbiage about what to do when more than one subelement appears (which has been done in the case of the new subelement, but not the old ones).; (2) .”

Options:

As presented in the mail message:

1. “Add prose requirements (not expressible in XSD) that subelements MUST appear a maximum of once in <Conditions> (the simplest);
2. “change <Conditions> backwards-incompatibly to contain an ordered list of 0..1 of each subelement (my favorite);
3. “add lots more SHOULD prose to the old subelement descriptions, similar to what's in the new one (yuck).”
4. (Not from the original mail message:) Use the XSD <all> feature to allow an unordered mixture of the condition elements, while controlling which ones are allowed to occur repeatedly vs. occur only once.

Resolution:

At the 11 May 2004 telecon we closed the issue, effectively choosing option #3: sticking to prose for any cardinality constraints.

CORE-18 KeyInfo as Special Case of Subject Confirmation Data (*Closed*)

Source:

2 March 2004 telecon: http://lists.oasis-open.org/archives/security-services/200403/msg00053.html

Owner:

Eve Maler

Description:

In this telecon it was noted that KeyInfo is allowed alongside the more general SubjectConfirmationData, but was intended to be a more-specific alternative to it. Should we put them in a choice group, or put more prose around them to explain what it means when both are present, or disallow them together just using prose?

Resolution:

It was decided at the March-April 2004 F2F to remove the explicit mention of KeyInfo, and explain that people should put this element *inside* SubjectConfirmationData whenever they want it.

CORE-19 Multiple Encryption Keys and Recipient Information (*Closed*)

Source:

March-April 2004 F2F

Owner:

Scott Cantor

Description:

The issue is whether or not we want to say anything about what you should put in XML Encryption's Recipient field to indicate the audience for the data. Do we say something like “Put a specific provider ID here”? This is similar to the Issuer situation, where we originally provided no guidance as to how to fill it in. This would be non-normative, but guidance could be helpful. This guidance should probably be in the general section about encryption, rather than specifically in the place(s) where <xenc:EncryptedKey> gets mentioned.

At the 11 May 2004 telecon, Scott noted that this issue is the motivator for putting something about "identifying system entities" in the core spec.

Resolution:

The spec now has wording around this.

CORE-20 Change AuthnContextStatement Element Name (*Closed*)

Source:

March-April 2004 F2F

Owner:

John Kemp

Description:

The Authentication Context spec defines an element called AuthnContextStatement, which appears as a descendant of a SAML statement element. This is confusing. Several renamings were suggested: AuthnContextClaim, ...Declaration, ...Pronouncement, etc.

Resolution:

We discussed it in the 27 April 2004 telecon and decided on AuthnContextDetail. John Kemp will review and implement this change in the core and authn context specs.

CORE-21 Consent vs. Reason (~~*Open*~~*Closed*)

Source:

March-April 2004 F2F

Owner:

Scott Cantor

Description:

The Reason attribute in the single logout protocol is weird. It overlaps with the top-level Consent attribute in some respects.

Resolution:

~~@@~~In the telecon of 13 July 2004, we decided to close this because recent updates to the core spec solved the problem with prose.

CORE-22 URIs vs. Prefixed QNames in Status Codes (*Closed*)

Source:

March-April 2004 F2F

Owner:

Scott Cantor

Description:

A potential problem was discovered in the SAML interop event held at the RSA 2004 conference: Although the SAML core spec requires there to be a namespace prefix on status code QNames, one vendor defaulted the prefix. Some have commented that it's inappropriate to require the prefix rather than allowing the natural XML namespace defaulting mechanism to be used, but others felt that since “QNames in content” are considered evil, it's hard to improve on its evilness around the edges. One possibility is to move away from a SOAP V1.1-like Qnames-in-content mechanism for status codes, and instead use URIs.

Note the WSS has actually made the switch to full URIs for status codes.

Resolution:

Scott has implemented a switch to URIs for status codes in rev core-15. In the 22 June 2004 telecon, we agreed to close this.

CORE-23 Review Element vs. Attribute Choices (*Open*)

Source:

March-April 2004 F2F

Owner:

@@

Description:

John Kemp noted that the pattern of element vs. attribute usage throughout the SAML schemas is not entirely consistent. We need to do a review and decide whether to sync up our usage. (We're doing this ad hoc.)

Resolution:

@@

CORE-24 Rename DoNotCacheCondition to OneTimeUseCondition (*Closed*)

Source:

March-April 2004 F2F

Owner:

Eve Maler

Description:

We discovered at the F2F that “one-time use” describes the semantic much more accurately.

Resolution:

At the 11 May 2004 telecon, we agreed to make the name change.

CORE-25 Require SessionIndex on LogoutRequest (*Closed*)

Source:

March-April 2004 F2F

Owner:

Scott Cantor

Description:

This was an outstanding question posed by John Kemp in his session-related work.

Resolution:

On the 22 June 2004 telecon, we agreed to document a meaning for an absent SessionIndex: Log out all sessions for a principal.

CORE-26 Consider Changing the Type of the IDPEntry Element's ID Attribute (*Closed*)

Source:

11 May 2004 telecon

Owner:

Scott Cantor

Description:

In the discussion of issue CORE-16, the question of why this attribute has a type of anyURI came up.

Options:

1. Leave the type alone.
2. Leave the type alone and be more specific about what URIs could go there.
3. Change the type to “ID”.
4. Change the type to something else.

Resolution:

The name has been changed to ProviderID, so this is closed.

CORE-27 Consider Limiting Datatype of Attribute Name (~~*Open*~~*Closed*)

Source:

1 June 2004 telecon

Owner:

@@

Description:

Prateek has been proposing a “simple attribute profile”, one of whose characteristics is to limit the Name field on the Attribute element to “xs:name”. This may be slightly too restrictive (it has to accommodate anyURI at a minimum), but maybe “xs:token” or something would be appropriate to do in core, so that all attribute profiles will inherit it (rather than having this one attribute profile do it).

Options:

@@

Resolution:

@@In the telecon of 13 July 2004, we decided to close this by adding language explaining that we have made a prose constraint here that goes beyond the XSD datatype chosen.

CORE-28 Resolve Conflict Between wsu:id and SAML Assertion ID (*Closed*)

Source:

Ron Monzillo email thread: http://lists.oasis-open.org/archives/security-services/200407/msg00076.html

Owner:

@@

Description:

The WSS TC has been discussing how best to reference SAML token, given that SAML has its own native ID attribute but some prefer using a standard ID attribute whose type is a priori known to be xsd:ID.

Options:

@@

Resolution:

At the telecon of 20 July 2004, we decided that the right course of action is to wait until there is a truly universal ID attribute available (the W3C's xml:id) and use that in whatever new version of SAML is being worked on.

2.2 BIND: Binding and Profile Issues

The following are issues related to the Technical Overview deliverable.

BIND-1 Disallow Status as Only Child of SOAP Body (*Closed*)

Source:

oasis-sstc-saml-bindings-1.1.pdf lines 316-317.

Owner:

Frederick Hirsch.

Description:

This impacts the bindings spec. Section 3.1.3.6, Error Reporting, needs to change to winnow the two choices for inclusion of a <Status> element in a SOAP message down to the recommended one, and mention that one method was removed.

Resolution:

This is a backwards-incompatible change decided and promised in the V1.0 timeframe but unable to be implemented until V2.0. Implemented in bindings-02.

BIND-2 Remove Deprecated Artifact URI (*Closed*)

Source:

oasis-sstc-saml-bindings-1.1.pdf line 426.

Owner:

Frederick Hirsch.

Description:

This impacts the bindings spec. Section 4.1.1.1, Required Information (for Browser/Artifact Profile of SAML), needs to change to remove the deprecated URI, and several subsequent subsections

need to be edited (search for the word “deprecated”) to remove mention of the deprecated option.

Resolution:

This is a backwards-incompatible change decided and promised in the V1.0 timeframe but unable to be implemented until V2.0. Implemented in bindings-02.

BIND-3 Establish a Mandatory Profile (*Open*)

Source:

Dan Blum of Burton Group in remarks on his weblog (http://www.burtongroup.com/weblogs/danielblum/archives/2003/11/000179.html) and subsequent private conversation. See also the continuing discussion on the TC list: http://lists.oasis-open.org/archives/security-services/200311/msg00027.html

Owner:

@@

Description:

Dan actually made several suggestions in his blog entry:

“1) OASIS, or an appropriate third party, should arrange for a reference implementation, or test harness, of SAML to be created against which all implementers can freely test over the network. This alone may be sufficient to solve the brunt of the interoperability issue, and it should be possible to create such an implementation using OpenSAML or SourceID in less than 90 days. As a follow up OASIS or an appropriate third party could also arrange for recurring interoperability testing events similar to those Liberty Alliance has announced.

“2) Since the majority of vendors we surveyed so far support unsigned SAML 1.0 requests using the artifact profile over SSL connections with client and server authentication, the test harness should support this use case ASAP, then the others. We also believe the SSTC should consider making the described use case mandatory so that all customers can be assured of a "lowest common denominator" SAML interaction mode regardless of the vendor they pick.

“3) In addition, customers are generally finding federated identity business issues difficult. OASIS should publish a "SAML cookbook" that customers can read to categorize their required pattern of federation, assess their risks, and compose a workable strategy going forward.“

This issue specifically relates to the second part of suggestion #2. His other suggestions are being taken up in other fashions: The co-chairs are looking into #1, and the editors are looking into #3 as an editorial matter. This is also related to conformance.

We discussed this at the 27 April 2004 telecon. We are going from two SSO profiles to one, so *if* someone is implementing SSO, the choice of a mandatory profile seems obvious! However, what Dan was probably going for was a choice between artifact and POST. It seems clear now that both have their place, and some in the TC are in favor of requiring both. This is still open.

Resolution:

@@

BIND-4 Representing attribute profiles in core and metadata (*Open*)

Source:

SAML telecon 22 June 2004

Owner:

@@

Description:

We need to figure out how to represent attribute profiles in the core and metadata specs.

Resolution:

@@

2.3 TECH: Other Technical Issues

The following are technical issues related to areas not already covered above.

TECH-1 Identity/Service Provider Terminology and Domain Model (*Closed~~Open~~*)

Source:

SAML F2F 22-24 October 2003.

Owner:

Eve Maler

Description:

Currently we introduce terminology in the bindings spec about “source” and “destination” sites, which we've never been entirely happy with. Liberty uses “identity provider” and “service provider”, which are more meaningful. (Note that “identity provider” is broader than “authentication authority”.) We need to consider a wholesale change to our terminology, either in the Liberty direction or in some other direction. The solution should be able to be used globally across the specs, and not be specific just to the bindings. (We will likely still need the “asserting party”/”relying party” terminology because it has a different purpose.)

At the March-April 2004 F2F, we agreed that this issue should also include the related issue of creating an overall “domain model” or similar conceptual model that encompasses the new features of SAML V2.0 in general, as well as the question of whether a SAML authority exactly equals an IdP.

Options:

The obvious options are:

1. Keep the current terminology.
2. Change it over to an identity provider/service provider frame of reference in just the bindings document
3. Change it over in both bindings and core
4. Change it to yet another set of terms.

Resolution:

@@In the telecon of 13 July 2004, we decided to close this issue because all the new profiles have switched their terminology in a cohesive fashion, and we don't need the old domain model diagram anymore (the Technical Overview will cover the concepts in a different fashion).

TECH-2 Versioning of Elements (*Closed*)

Source:

Ongoing issue.

Owner:

Eve Maler

Description:

We need to decide whether to support mixing, say, older-version assertions inside newer-version responses. The current relationship between the protocol and assertion schemas is relatively static regarding version association. This was discussed at the March-April 2004 F2F, and the tentative conclusion was that, since assertions have such a relatively short lifetime, it shouldn't be necessary to allow for mixing of (e.g.) old assertions with new wrappers. However, we haven't made a formal decision on this matter yet.

Options:

There are two obvious choices: keep the versions in lockstep, or allow them to float.

Resolution:

We agreed to keep them in lockstep, and to document this fact in our Versioning section. Eve will develop some wording for this.

TECH-3 Impersonation Using SubjectConfirmation and KeyInfo (*Closed*)

Source:

SAML F2F meeting 3-5 February 2004, message thread from Ron Monzillo starting at http://lists.oasis-open.org/archives/security-services/200402/threads.html, and other threads in that month (http://lists.oasis-open.org/archives/security-services/200402/threads.html)

Owner:

@@

Description:

Ron says:

```
676: <ds:KeyInfo> [Optional]
676: An XML Signature [XMLSig] element that provides access to a cryptographic key
held by the subject.

The wss stp attempts to describe a holer-of-key impersonation model, where the
entity that confirms knowledge of the key is other than the subject of the assertion.

IMO, the text in SAML core, should be changed to say something like:

676: An XML Signature [XMLSig] element that identifies a cryptographic key that must
be demonstrated to satisfy the confirmation method.
```

And then:

```
In looking at this further, I now think that SAML CORE should not say
anything about the semantics of the data in keyInfo. These semantics should be
defined as part of the definition of the specific confirmation methods. I still
believe lines 676-677 should change, but I now think they should be changed to
say the following:

677: An XML Signature [XMLSig] element that identifies a cryptographic key.

Furthur, I think we should take a closer look at what the SAML BIND says about hok
863 5.1 Holder of Key
864 URI: urn:oasis:names:tc:SAML:1.0:cm:holder-of-key
865 A <ds:KeyInfo> element MUST be present within the <SubjectConfirmation> element.
866 As described in [XMLSig], the <ds:KeyInfo> element holds a key or information that
enables an
867 application to obtain a key. The subject of the statement(s) in the assertion is
the party that can
868 demonstrate that it is the holder of the key.

I can guess the intent of the last sentence, but it seems to me that its interpretion
depends on what one thinks was meant by the 2 uses of "is" in this sentence.

For example, the party that can demonstrate ... the key "is" the subject of the
assertion; as in, is to be recognized as the subject, vs. must be the subject.
```

Resolution:

The first half has been fixed through changes to the core spec; the Holder of Key issue (affecting the profiles spec) is still open. Ron has reviewed the profiles spec wording and thinks it's acceptable, so we formally closed this on the 22 June 2004 telecon.

TECH-4 Glossary Additions: Artifact, Binding, Profile (*Open*)

Source:

Jeff Hodges and others in message thread starting at http://lists.oasis-open.org/archives/security-services/200402/msg00061.html

Owner:

Rob Philpott

Description:

These terms are not formally defined, and in fact there is some vagueness around “profile”.

Options:

@@

Resolution:

@@Bindings are now better characterized. We need a proposal around profiles.

TECH-5 Improve Federation Terminology (*Open*)

Source:

March-April 2004 F2F

Owner:

@@

Description:

@@

Resolution:

@@

TECH-6 Highlight Privacy Considerations (*Open*)

Source:

March-April 2004 F2F

Owner:

@@

Description:

Rather than implicitly assume that privacy is always a goal, the specs should explicitly call out which design features exist to support privacy considerations.

Resolution:

@@

TECH-7 Add/Correct Instance Examples (*Open*)

Source:

March-April 2004 F2F

Owner:

@@

Description:

It has been a longstanding complaint that we don't provide XML instance examples in the core spec (though now we have a single complete example in the XML Signature section as of V1.1). We certainly need to update the example that's in there, and we need to consider adding examples either throughout the core spec or in the technical overview, or both.

Resolution:

@@

TECH-8 Create WSDLs for SAML Protocols (*Deferred*)

Source:

Eve Maler email: http://lists.oasis-open.org/archives/security-services/200407/msg00102.html

Owner:

@@

Description:

"Now that we've completed the "top-typing" process and the protocols all have distinct request-response element pairs, having a WSDL for each might be more handy. Are we interested in creating WSDLs this time around? If we do, would they be informative (maybe going in the Tech Overview?) or normative (possibly being provided/reference as part of each profile)? If we want these, is there anyone who's interested in creating them? "

Resolution:

This was discussed in the telecon of 20 July 2004. It is considered optional, and is not planned as a V2.0 deliverable. If someone wants to step up to create these after the V2.0 timeframe, it can go forward.

A. Acknowledgments

The editors would like to acknowledge the contributions of the OASIS Security Services Technical Committee, whose voting members at the time of publication were:

@@TBS

B. Revision History

Rev	Date	By Whom	What
01	13 Oct 2003	Eve Maler	Initial draft.
02	20 Oct 2003	Eve Maler	Marked CORE-1 through CORE-4 and BIND-1 through BIND-2 as closed because they have been implemented. Added CORE-6.
03	26 Oct 2003	Eve Maler	Added CORE-7, CORE-8, TECH-1, and TECH-2.
04	21 Nov 2003	Eve Maler	Added CORE-9 and BIND-3.
05	22 Dec 2003	Eve Maler	Added CORE-10 (and promptly closed it).
06	10 Feb 2004	Eve Maler	As a result of the F2F on 3-5 February 2004 and related discussions, added CORE-11 through CORE-15 and TECH-3 through TECH-4.
07	15 Mar 2004	Eve Maler	Added CORE-16 through CORE-18. Closed CORE-5. Edited CORE-6 and CORE-9, which are nearly resolved.
08	2 Apr 2004	Eve Maler	Closed CORE-6, CORE-15, CORE-13, and CORE-18. As a result of the March-April 2004 F2f, added CORE-19 through CORE-23 and TECH-4 through TECH-6.
09	27 Apr 2004	Eve Maler	Closed CORE-11, CORE-20, and TECH-2. Added CORE-24 and CORE-25 (proposed to be prio-B) and TECH-7 (proposed to be prio-C). Moved the ball a few yards on several other issues. Started using the 2004 version of the OASIS logo on the title page.
10	13 May 2004	Eve Maler	Closed CORE-14 and CORE-17. Added CORE-26 (proposed to be lower-prio). The current list of higher-prio issues is: CORE-16, CORE-24, CORE-25, TECH-1, TECH-4.
11	1 Jun 2004	Eve Maler	Removed unused blocks of issue types (didn't leave in the change-bars for this; too confusing). Closed CORE-8, CORE-19, CORE-24, and CORE-26. Added CORE-27.
12	29 Jun 2004	Eve Maler	Closed CORE-7, CORE-12, CORE-16, CORE-22, CORE-25, and TECH-3. Added BIND-4.
13	20 Jul 2004	Eve Maler	Closed CORE-9 (Wildcarding and Extensibility in the SAML Schemas), CORE-21 (Consent vs. Reason), CORE-27 (Consider Limiting Datatype of Attribute Name), TECH-1 (Identity/Service Provider Terminology and Domain Model). Added (and promptly closed) CORE-28 (Resolve Conflict Between wsu:id and SAML Assertion ID). Added (and promptly deferred) TECH-8 (Create WSDLs for SAML Protocols).

C. Notices

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS's procedures with respect to rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification, can be obtained from the OASIS Executive Director.

OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to implement this specification. Please address the information to the OASIS Executive Director.